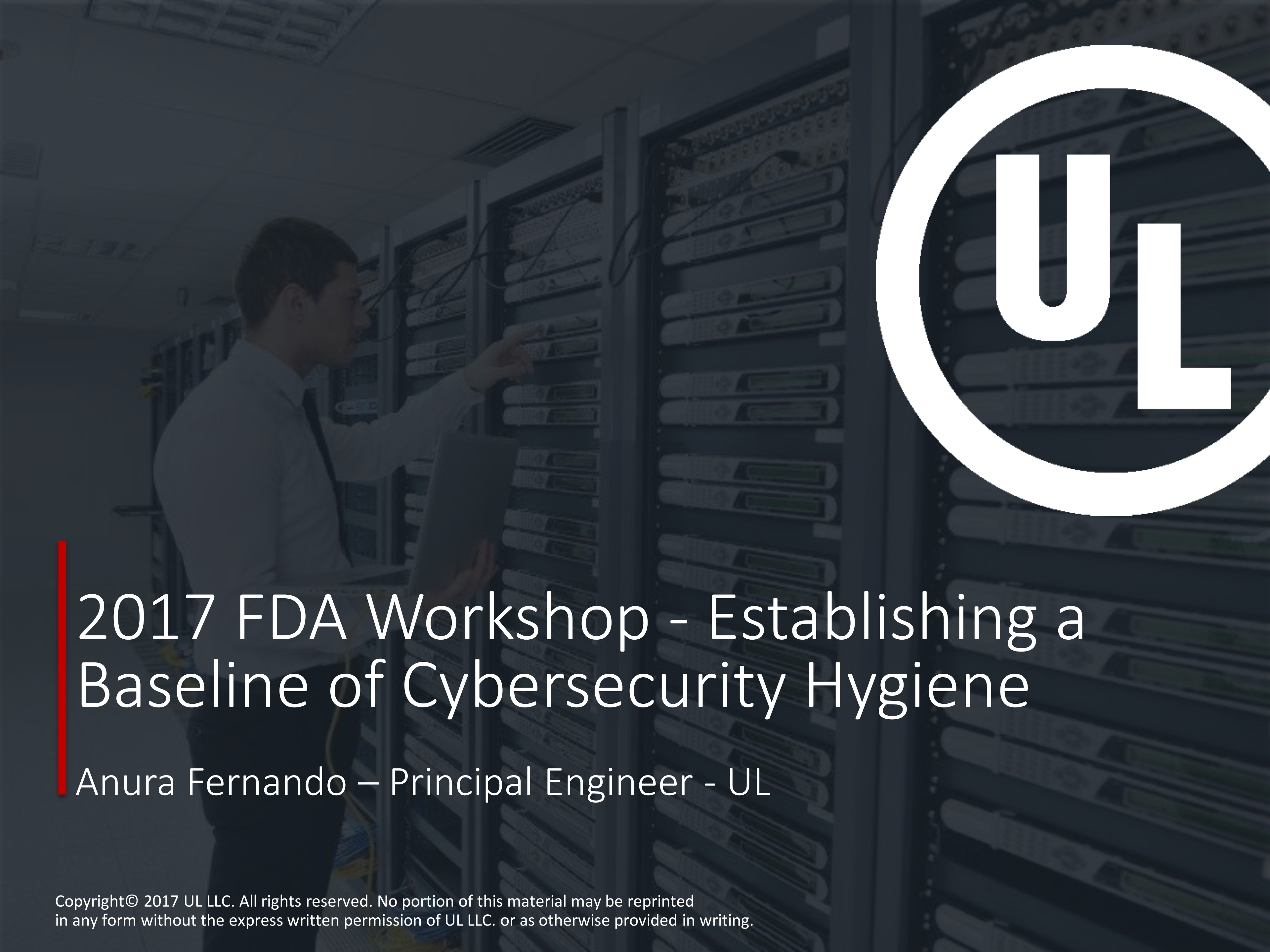
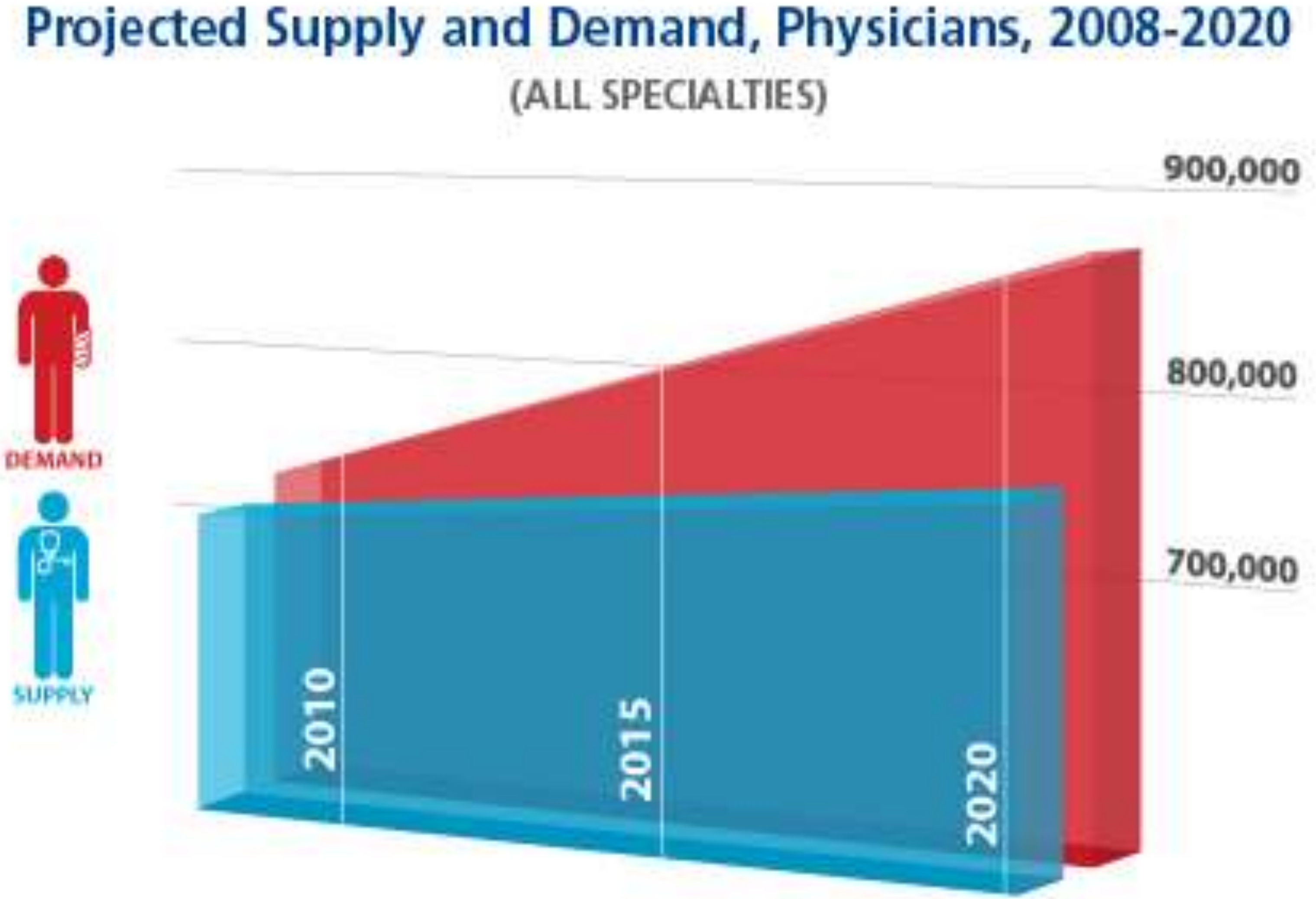


2017 FDA Workshop - Establishing a Baseline of Cybersecurity Hygiene

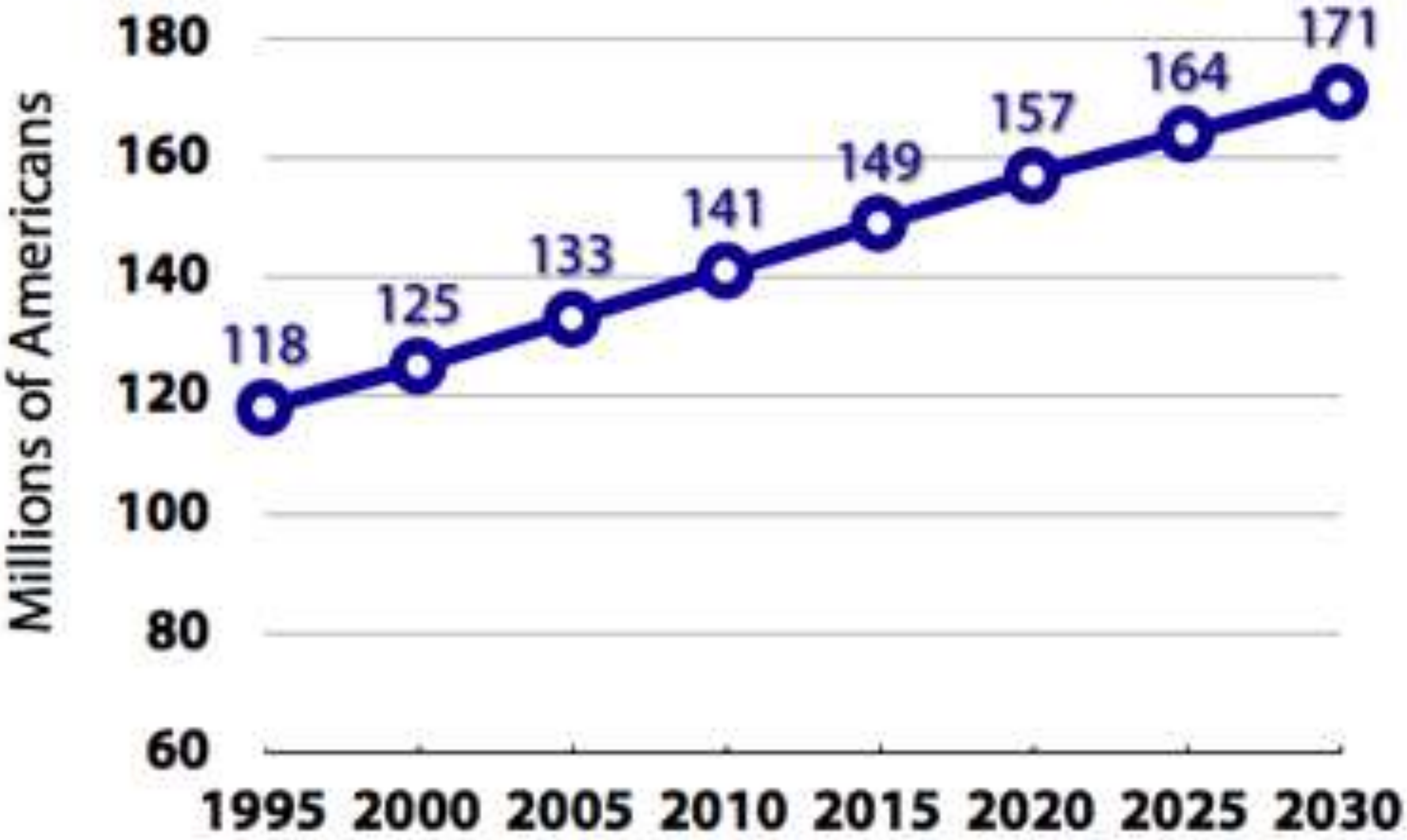
Anura Fernando – Principal Engineer - UL

Why are we really here today?



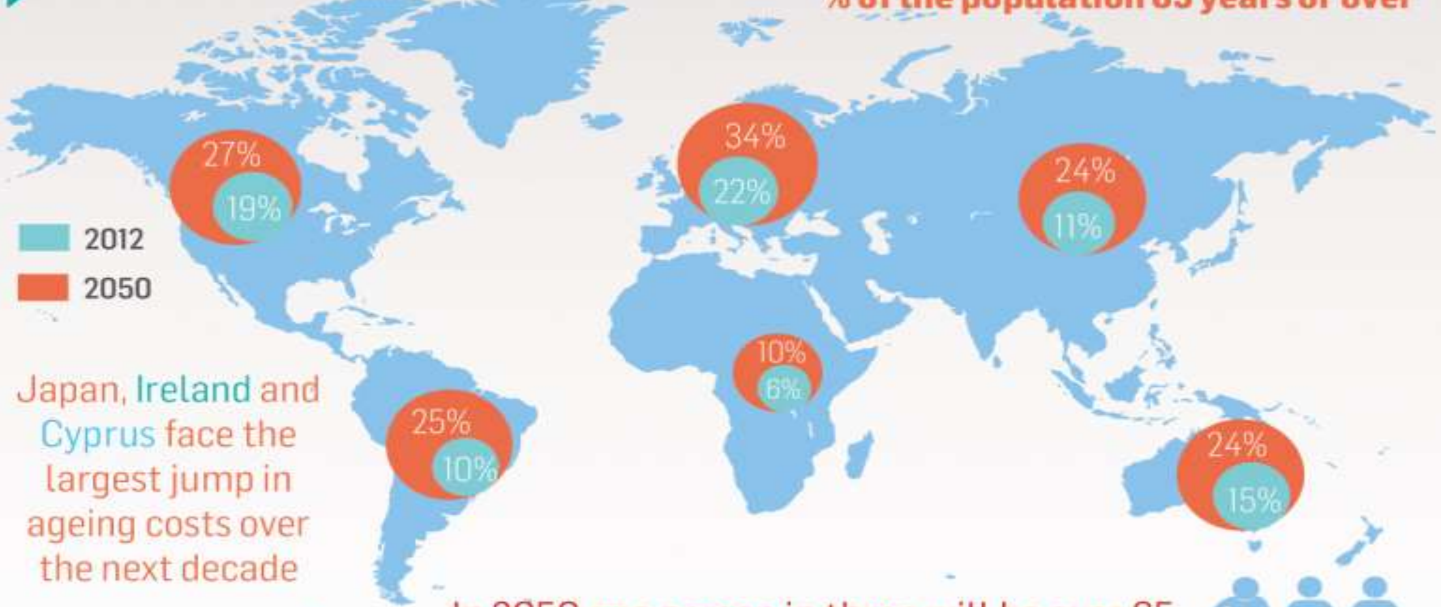
https://www.aamc.org/advocacy/campaigns_and_coalitions/fixdocshortage/

Prevalence of Chronic Disease in the U.S.



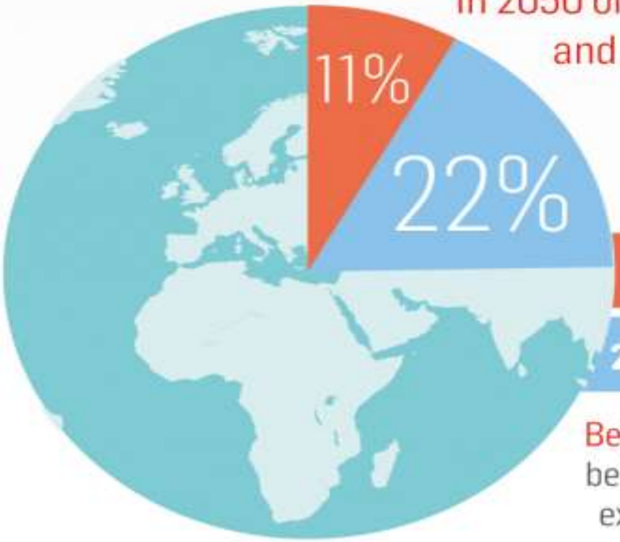
Source: Wu, Shin-Yi *et al*. 2000. Projection of Chronic Illness Prevalence and Cost Inflation. RAND Corporation.

THE WORLD'S AGEING POPULATION



Japan, Ireland and Cyprus face the largest jump in ageing costs over the next decade

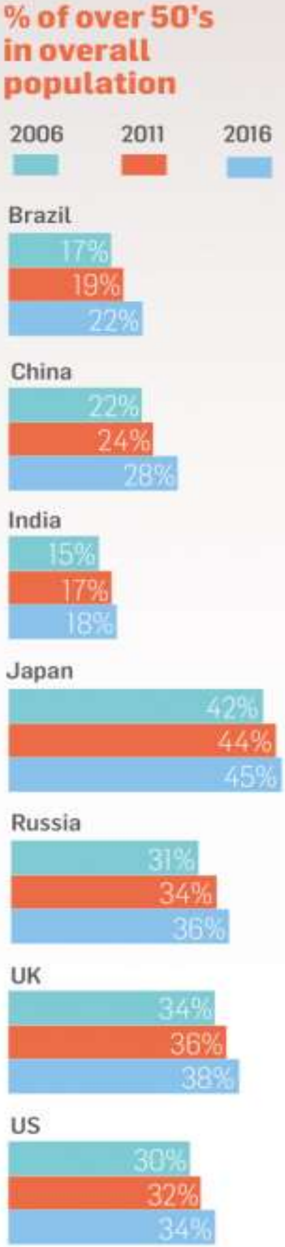
In 2050 one person in three will be over 65 and one person in ten will be over 80



2012 - 11% of the world's 6.9bn people are over 60

2050 - 22% of the world's 9bn people will be over 60

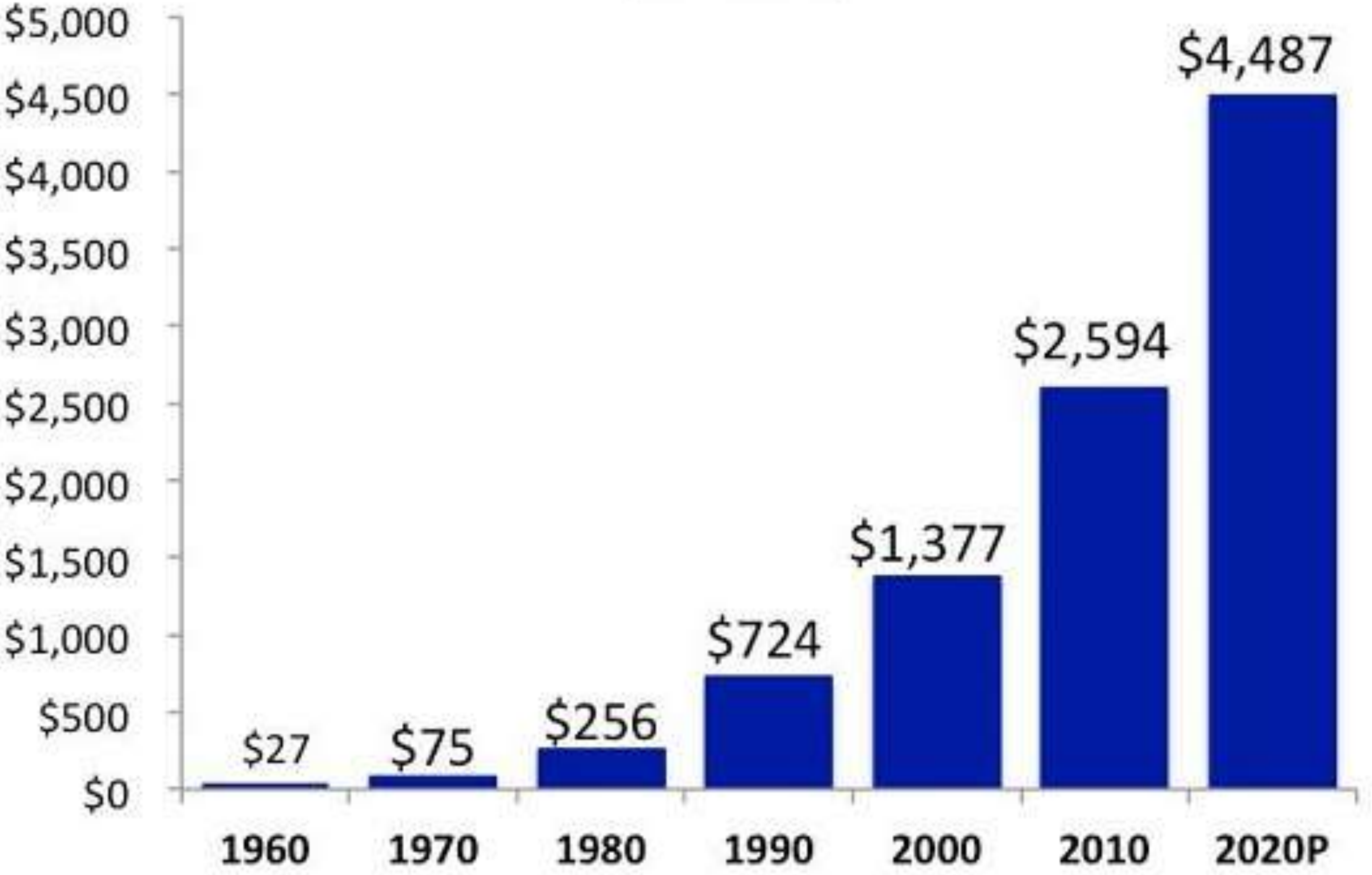
Between now and 2050 the fiscal burden of the crisis will be 10% of the ageing-related costs. The other 90% will be extra spending on pensions, health and long-term care



http://prafulla.net/interesting-contents/world-interesting-contents/the-worlds-ageing-population-infographic/

Healthcare Costs 1960 – 2020

(In Billions)



Centers for Medicare and Medicaid Services 2012 California Healthcare Foundation

How do we fix this problem?

One approach has been through the use of computing technologies

http://intpmcomms.com/wp-content/uploads/2010/08/iStock_000011296304XSmall1.jpg

…that can be found everywhere

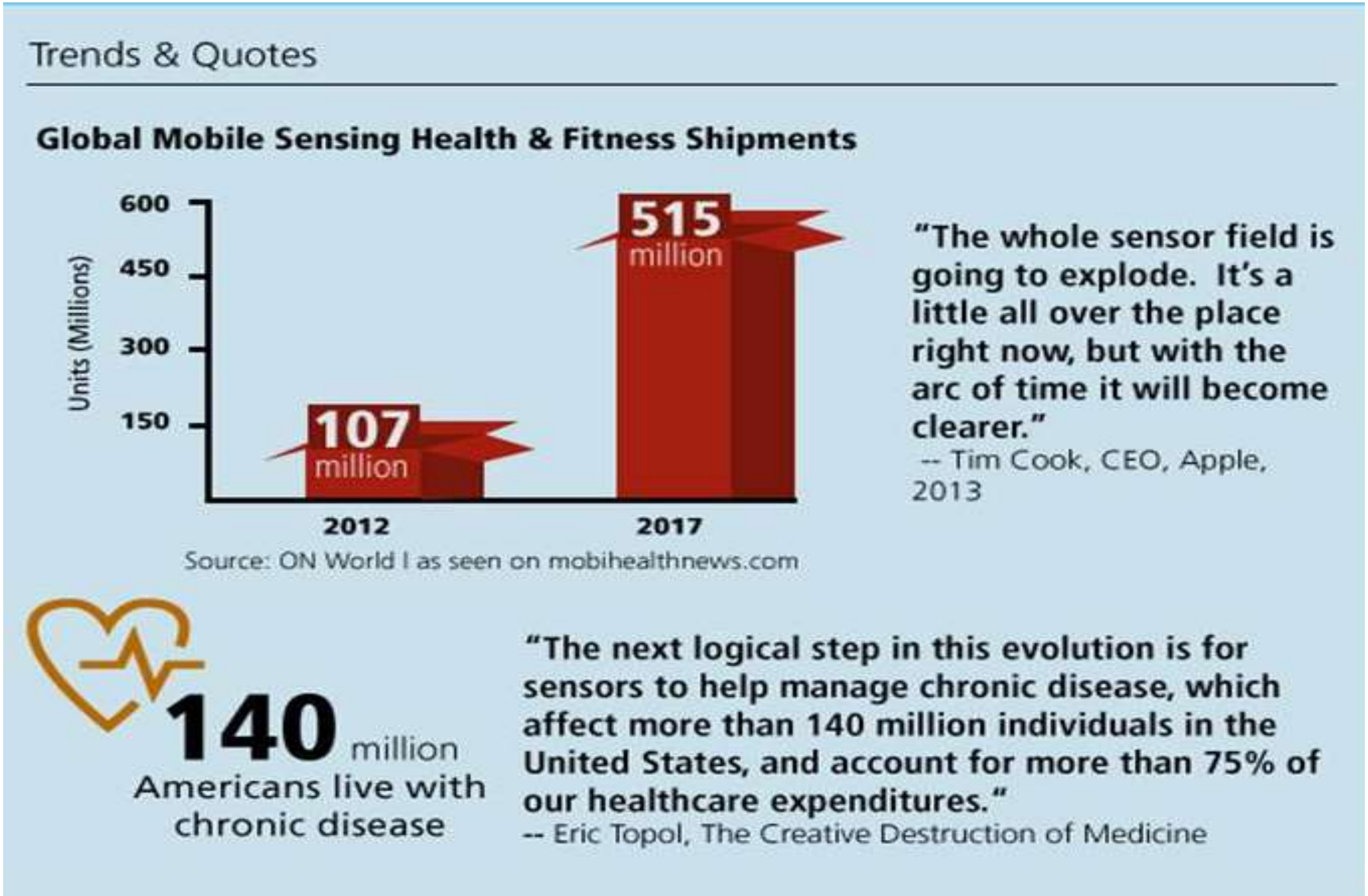
http://2.bp.blogspot.com/-afr-gp6eyl

http://www.theverge.com/2013/4/26/4268982/idc-q1-2013-smartphone-market-data

http://www.untitledname.com/archives/upload/2005/10/bicyclist-cell-phone.jpg

http://thecoolgadgets.com/

Cheaper and better sensors make this viable



Trends & Quotes

Global Mobile Sensing Health & Fitness Shipments

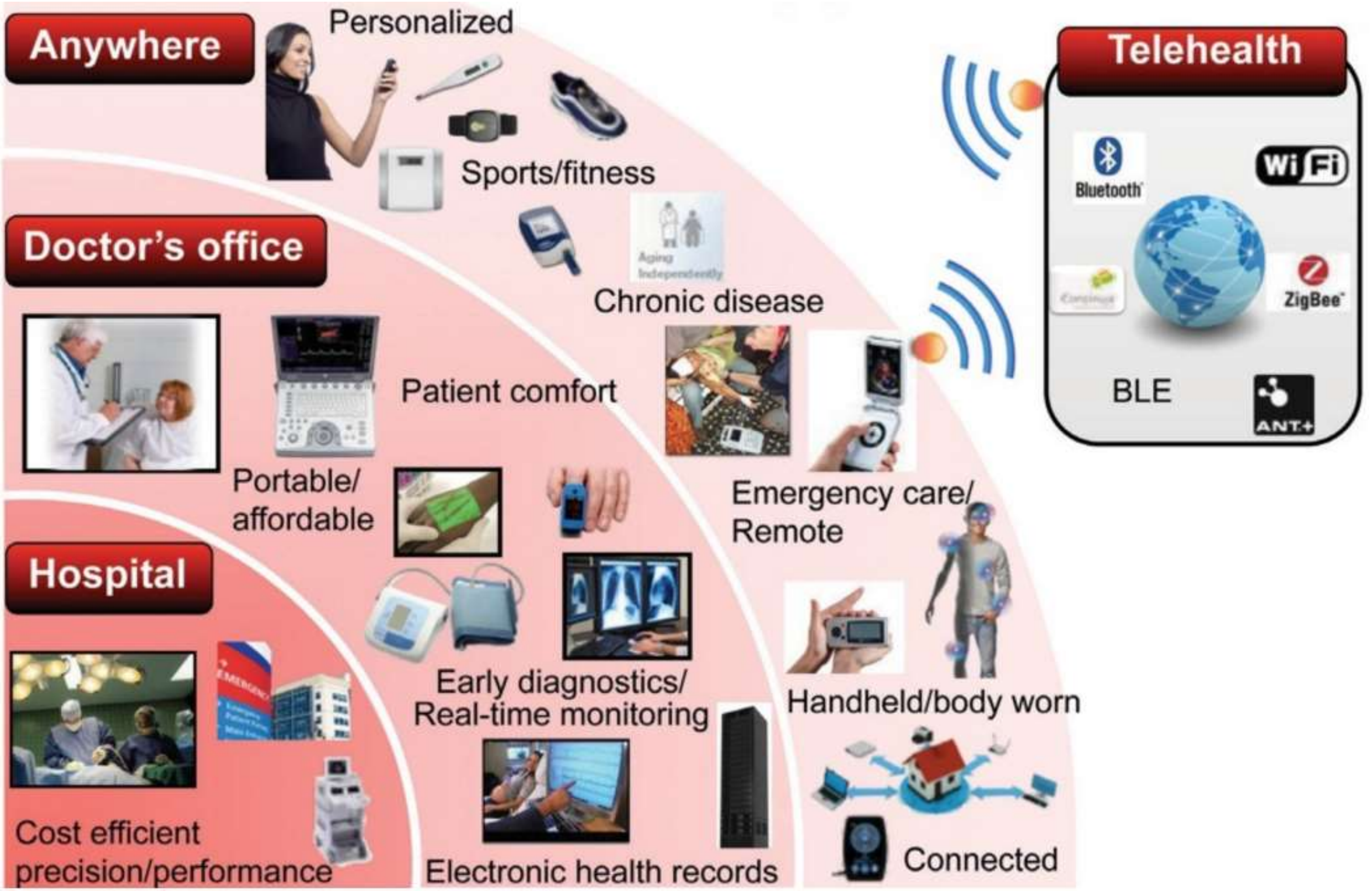
Source: ON World I as seen on mobihealthnews.com

“The whole sensor field is going to explode. It’s a little all over the place right now, but with the arc of time it will become clearer.”
-- Tim Cook, CEO, Apple, 2013

140 million Americans live with chronic disease

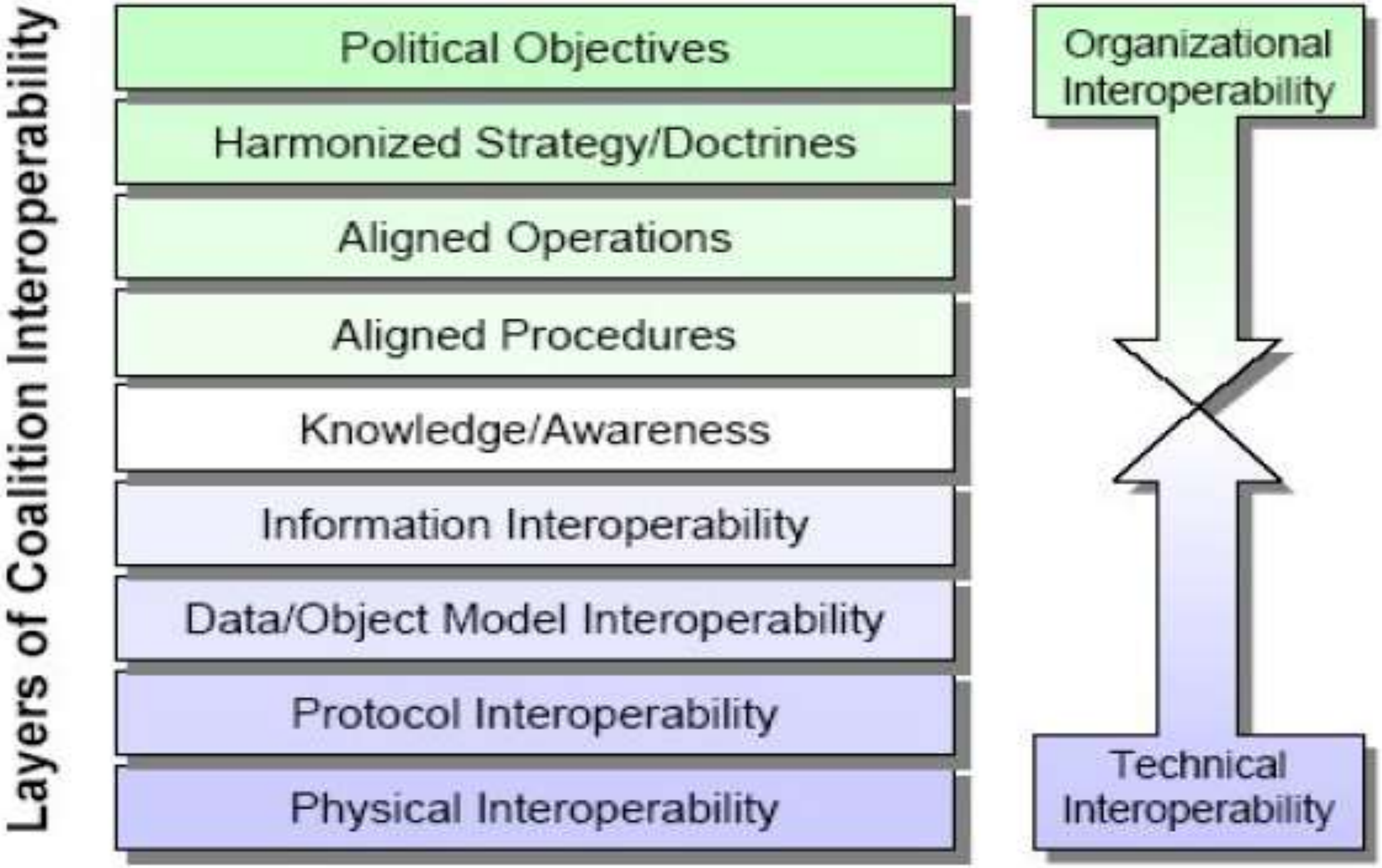
“The next logical step in this evolution is for sensors to help manage chronic disease, which affect more than 140 million individuals in the United States, and account for more than 75% of our healthcare expenditures.“
-- Eric Topol, The Creative Destruction of Medicine

Innovation leads to new ways to provide healthcare with limited clinician resources



Source: TI Medical

“Interoperability” is a key to success of this approach



Layers of Coalition Interoperability
Political Objectives
Harmonized Strategy/Doctrines
Aligned Operations
Aligned Procedures
Knowledge/Awareness
Information Interoperability
Data/Object Model Interoperability
Protocol Interoperability
Physical Interoperability
Organizational Interoperability
Technical Interoperability

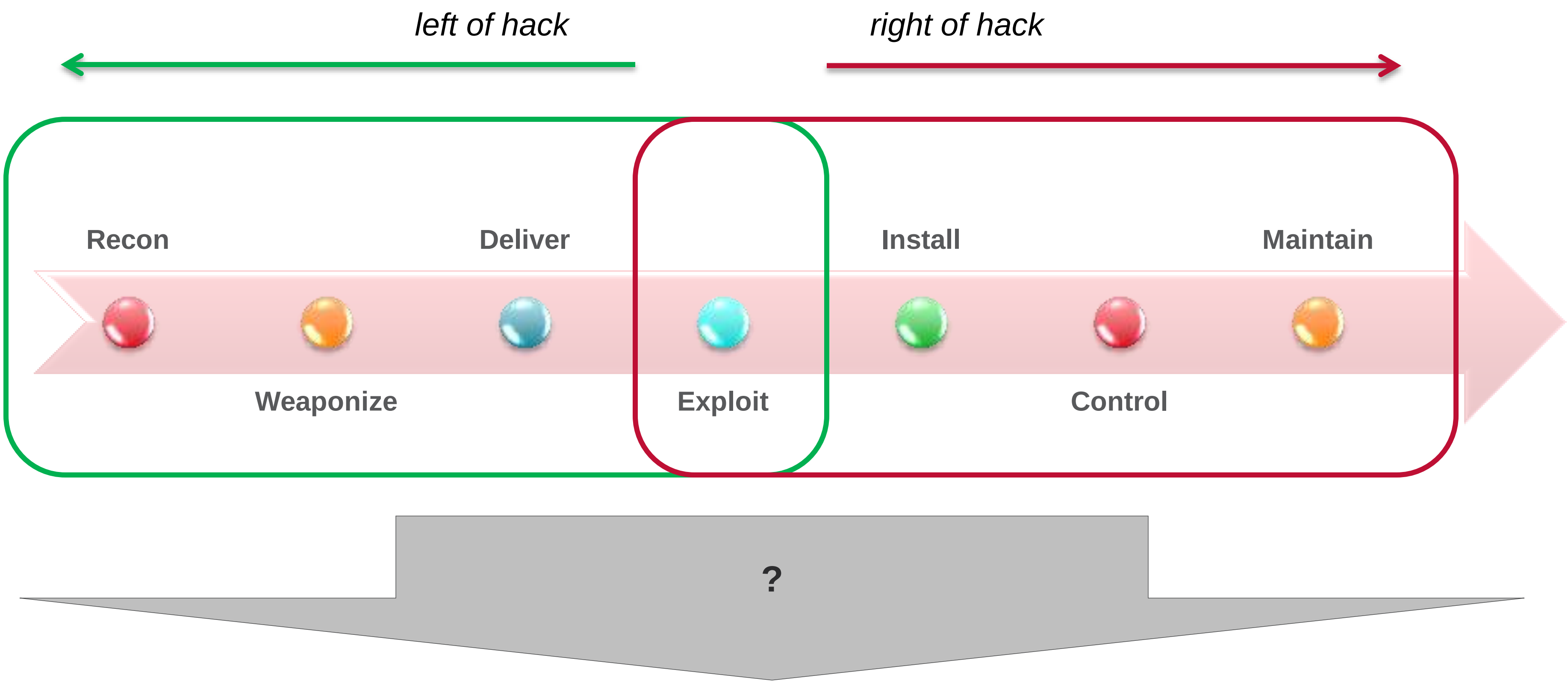
[Tolk 03] Tolk, Andreas. “Beyond Technical Interoperability – Introducing a Reference Model for Measures of Merit for Coalition Interoperability.” 8th International Command and Control Research and Technology Symposium (ICCRTS), Washington, D.C., June 17-19, 2003. Washington DC: Command and Control Research Program (CCRP), 2003

Problem solved !

So, why are we here again ???

New (mis)use cases that are reasonably foreseeable

How an attack works and potentially affects safety



Potential Failure Mode	Potential Causes	Potential Effects	Existing Controls	SEV	OCC	RPN	Risk Control Measures	SEV	OCC	RPN	Record of Mitigation	Any New Risk / Hazard Created?	Risk Reduced As Far As Possible?

“Big data” trends create a richer pool of targets

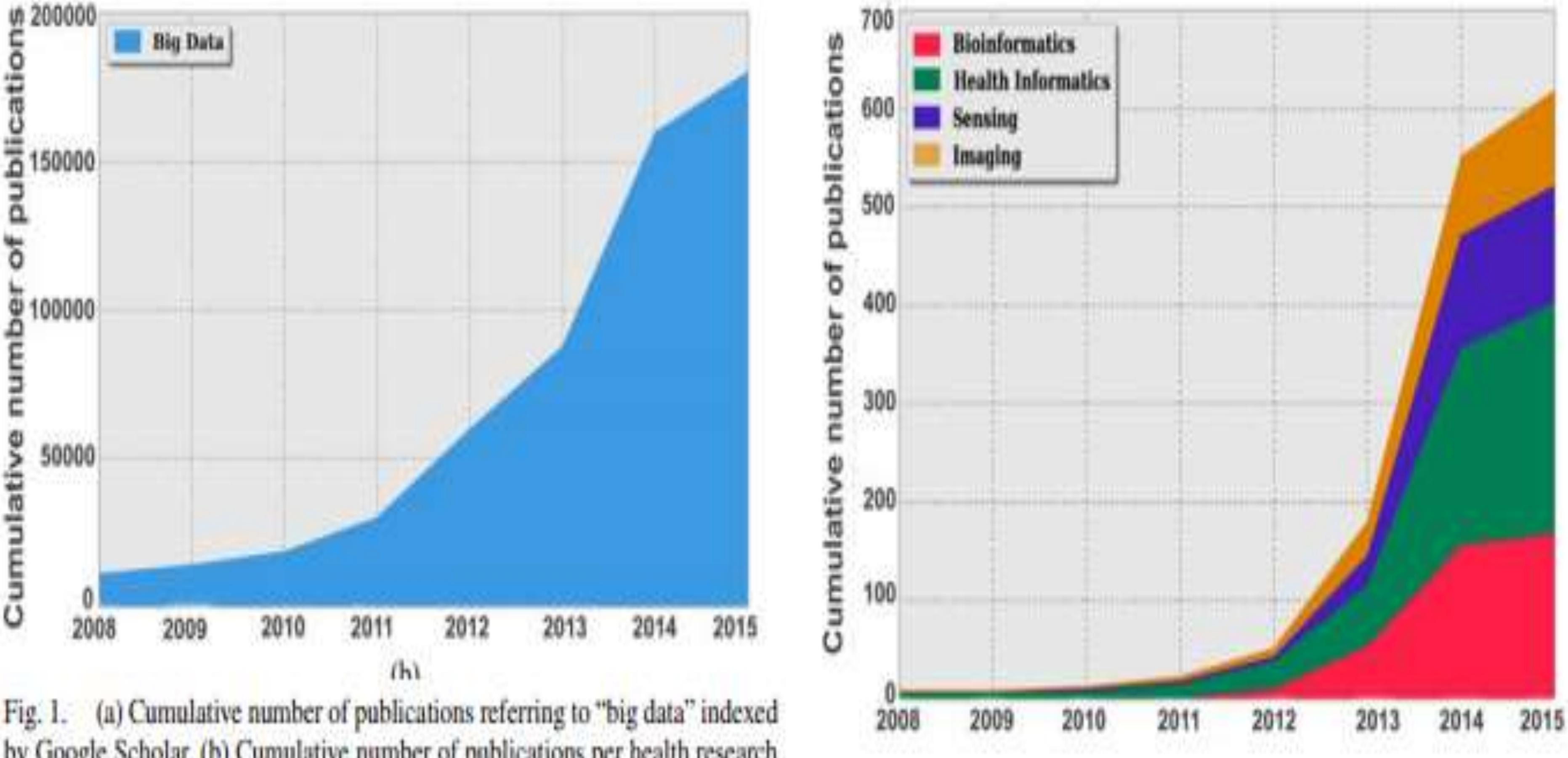
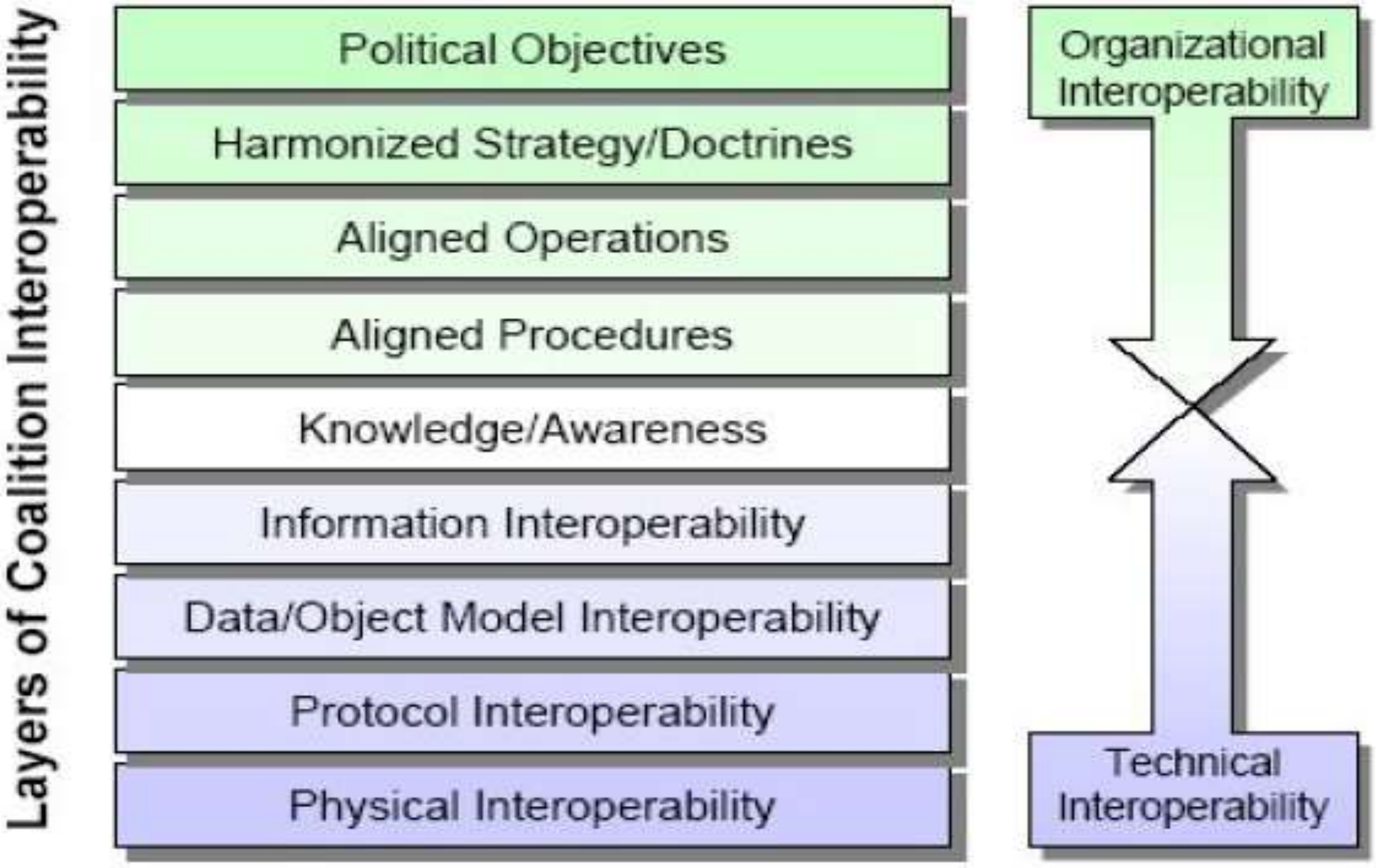


Fig. 1. (a) Cumulative number of publications referring to “big data” indexed by Google Scholar. (b) Cumulative number of publications per health research area referring to “big data,” as indexed in IEEE Xplore, ACM Digital library, PubMed (National Library of Medicine, Bethesda, MD), Web of Science, and Scopus.

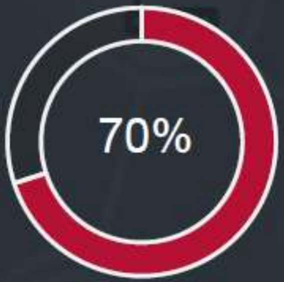
http://healthitanalytics.com/news/understanding-the-growth-value-of-healthcare-big-data-analytics

Where do hackers find vulnerabilities to exploit?

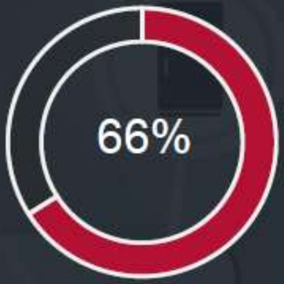

Layers of Coalition Interoperability
Political Objectives
Harmonized Strategy/Doctrines
Aligned Operations
Aligned Procedures
Knowledge/Awareness
Information Interoperability
Data/Object Model Interoperability
Protocol Interoperability
Physical Interoperability
Organizational Interoperability
Technical Interoperability

[Tolk 03] Tolk, Andreas. "Beyond Technical Interoperability – Introducing a Reference Model for Measures of Merit for Coalition Interoperability." 8th International Command and Control Research and Technology Symposium (ICCRTS), Washington, D.C., June 17-19, 2003. Washington DC: Command and Control Research Program (CCRP), 2003

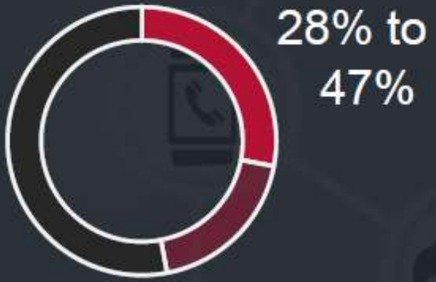
The IoT Cyber Threat



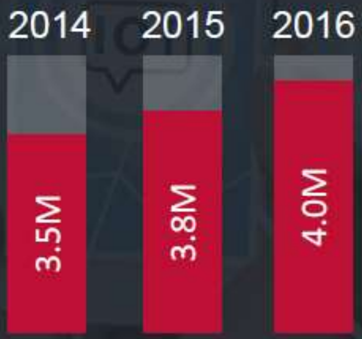
70% of IoT devices are vulnerable to attack *(Source:HP)*



By 2018, 66% of networks will have experienced an IoT security breach *(Source: IDC Research)*



28% to 47% of organizations have experienced IoT-related breaches *(Source: Forrester/CISCO)*



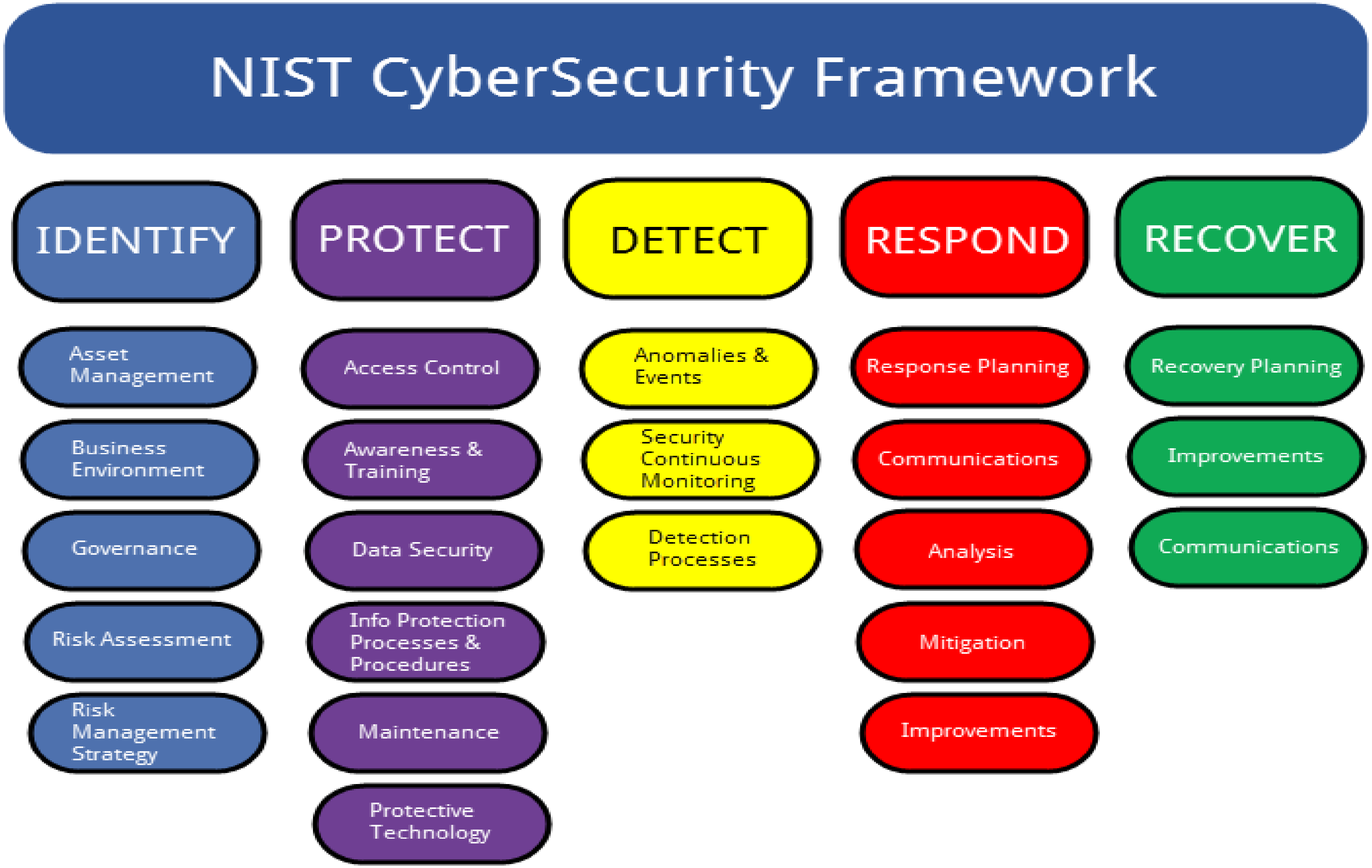
In 2016, the average consolidated total cost of a data breach was $4M USD *(Source: 2016 Ponemon Study)*

What’s different about healthcare?

- Patient safety is the most important “asset”
- It is not an issue of just individual patients but also whole populations of patients
- Product risk profiles can be very diverse making risk factors difficult to normalize (e.g. some medical products intentionally expose people to radiation)
- Medical IoT and Telehealth are moving elements of the “practice of medicine” from the hospital into the home.

Where do we start when trying to tackle these problems?

Apply

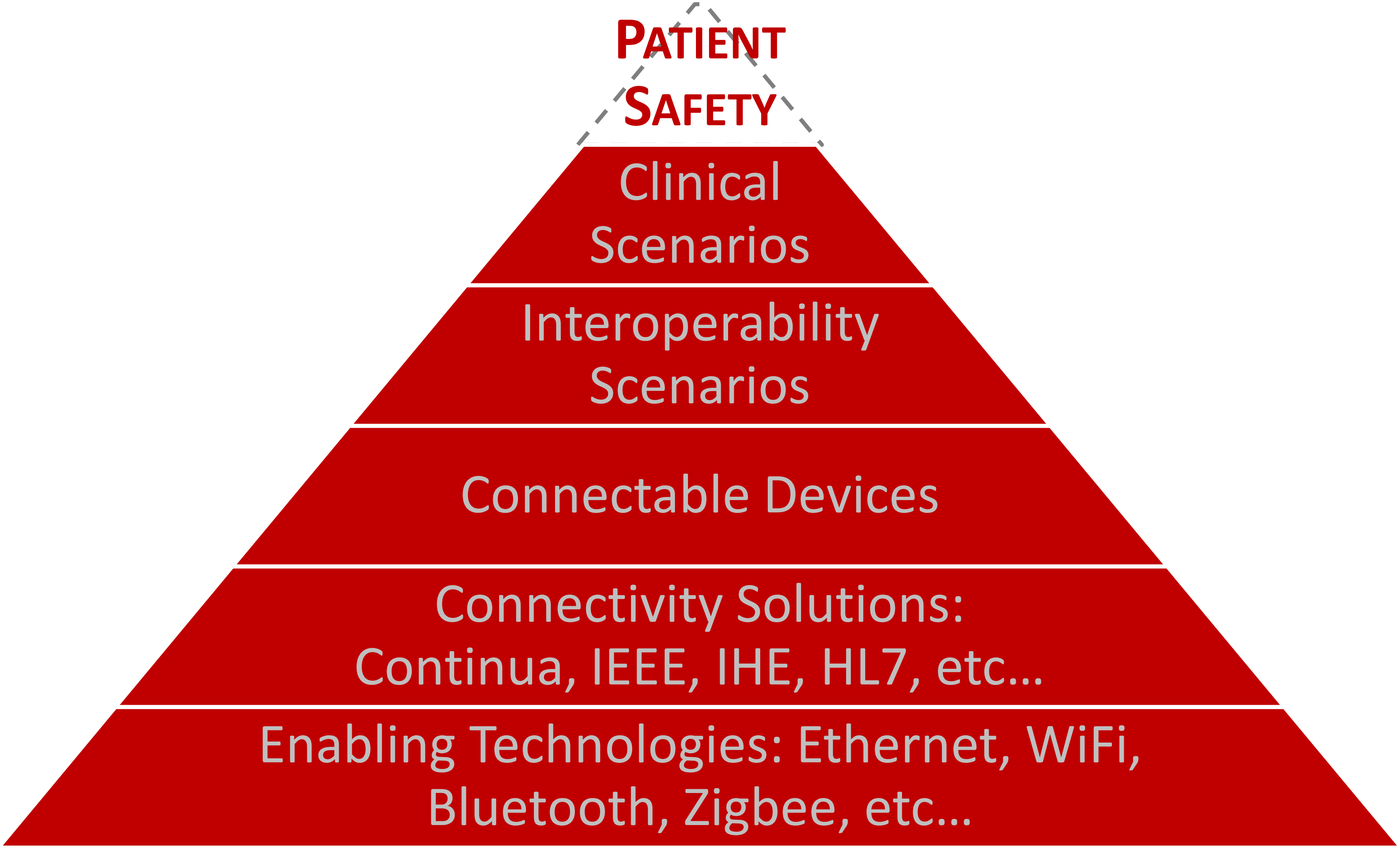


NIST CyberSecurity Framework

IDENTIFY	PROTECT	DETECT	RESPOND	RECOVER
Asset Management	Access Control	Anomalies & Events	Response Planning	Recovery Planning
Business Environment	Awareness & Training	Security Continuous Monitoring	Communications	Improvements
Governance	Data Security	Detection Processes	Analysis	Communications
Risk Assessment	Info Protection Processes & Procedures		Mitigation	
Risk Management Strategy	Maintenance		Improvements	
	Protective Technology			

Source: XlentSoftware

Analyze
the sociotechnical system



PATIENT SAFETY

Clinical Scenarios

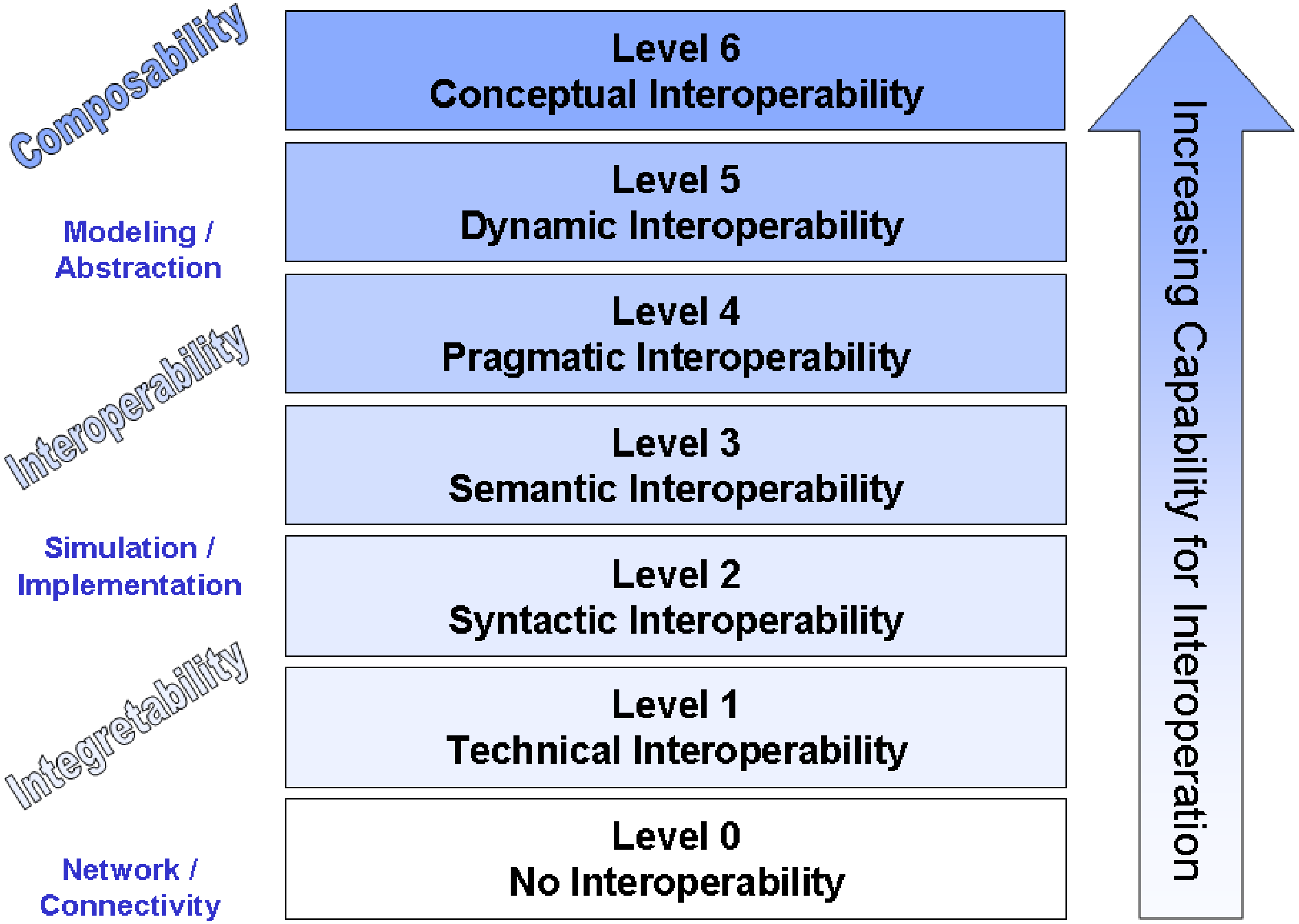
Interoperability Scenarios

Connectable Devices

Connectivity Solutions: Continua, IEEE, IHE, HL7, etc…

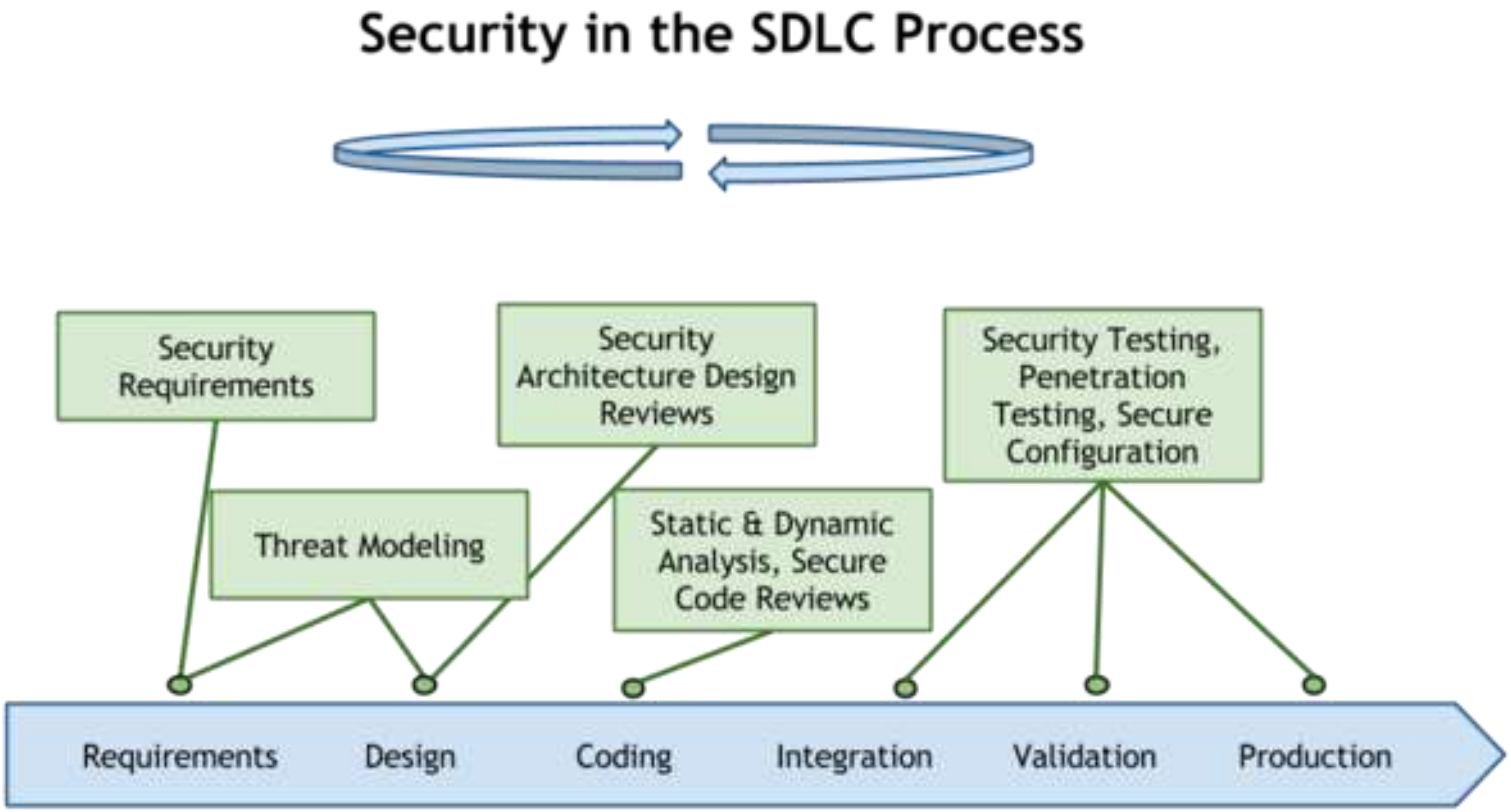
Enabling Technologies: Ethernet, WiFi, Bluetooth, Zigbee, etc…

How might interoperability be exploited?


Composability
Modeling / Abstraction
Interoperability
Simulation / Implementation
Integretability
Network / Connectivity
Level 6
Conceptual Interoperability
Level 5
Dynamic Interoperability
Level 4
Pragmatic Interoperability
Level 3
Semantic Interoperability
Level 2
Syntactic Interoperability
Level 1
Technical Interoperability
Level 0
No Interoperability
Increasing Capability for Interoperation

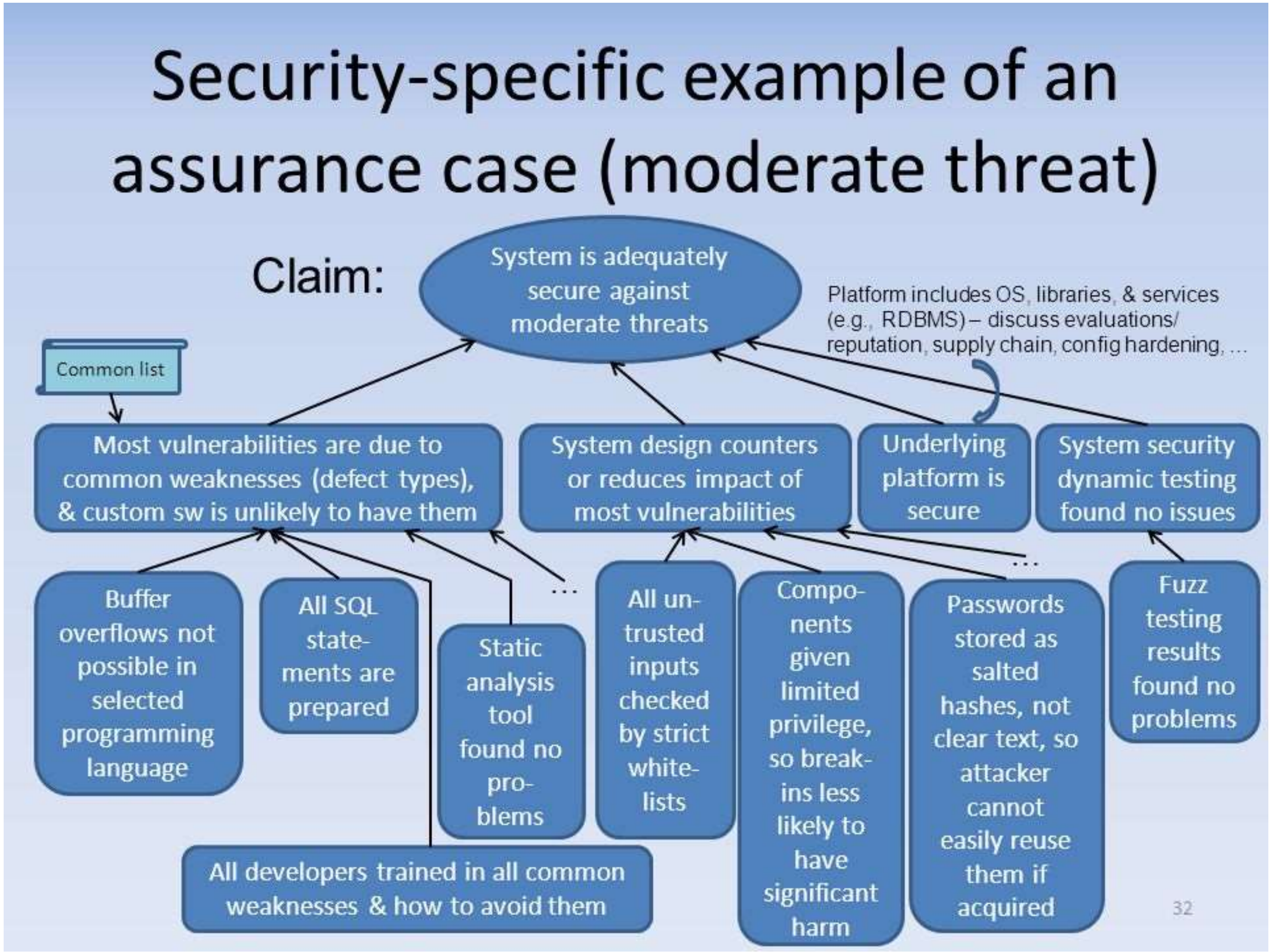
https://en.wikipedia.org/wiki/Conceptual_interoperability#/media/File:LCIM.png

Build security In


Security in the SDLC Process
Security Requirements
Threat Modeling
Security Architecture Design Reviews
Static & Dynamic Analysis, Secure Code Reviews
Security Testing, Penetration Testing, Secure Configuration
Requirements
Design
Coding
Integration
Validation
Production

http://2.bp.blogspot.com/-7Hr15ZJhi34/VnPYDOITxtI/AAAAAAAAETQ/hU7uJxEQEik/s640/600px-Security_in_the_SDLC_Process.png

Show evidence of security claims



Security-specific example of an assurance case (moderate threat)

Claim: System is adequately secure against moderate threats

Platform includes OS, libraries, & services (e.g., RDBMS) – discuss evaluations/ reputation, supply chain, config hardening, …

Common list

Most vulnerabilities are due to common weaknesses (defect types), & custom sw is unlikely to have them

System design counters or reduces impact of most vulnerabilities

Underlying platform is secure

System security dynamic testing found no issues

Buffer overflows not possible in selected programming language

All SQL statements are prepared

Static analysis tool found no problems

…

All untrusted inputs checked by strict whitelists

Components given limited privilege, so break-ins less likely to have significant harm

Passwords stored as salted hashes, not clear text, so attacker cannot easily reuse them if acquired

…

Fuzz testing results found no problems

All developers trained in all common weaknesses & how to avoid them

32

http://slideplayer.com/slide/678947/1/images/32/Security-specific+example+of+an+assurance+case+(moderate+threat).jpg

Many standards and guidance documents are available to help meet different objectives

Guidance Documents

- ISO/IEC TR 15443
- ITU-T CYBEX 1500 series
  - CVE / NVD
  - CWE (CWRAF/ CWSS, SANS CWE Top 25 / OWASP Top 10) and CAPEC
- ISO/IEC 27000 series
- ISO/IEC 15408
- ISO/IEC DIS 20243 /O-TTPS
- FISMA
- HIPAA
- IEC 62443
- DTSec
- IEC 80001
- AAMI TIR 57
- PCI
- SANS 20 CSC
- Cyber Essentials (UK)
- US FDA Pre- and Post- Market Guidance
- UL 2900
- Top 35 mitigation strategies (AU)
- NIST Cybersecurity Framework & SP 800-53r4 security controls
- DHS C^3 VP & CRR
- SAE AS5553 & 6174

Example – UL 2900
criteria for a baseline of cybersecurity hygiene focused on repeatable reproducible testing

UL 2900

- Fuzz Testing
- Known Vulnerability
- Code & Binary Analysis
- Access Control & Authentication
- Cryptography
- Remote Communication
- Software Updates
- Risk Assessment
- Structured Pen Testing

Fuzz Testing

A technique used to discover coding errors and security loopholes in software, operating systems, or networks by inputting massive amounts of random data, called fuzz, in an attempt to make the device operate improperly.

UL 2900

- Fuzz Testing
- **Known Vulnerability**
- Code & Binary Analysis
- Access Control & Authentication
- Cryptography
- Remote Communication
- Software Updates
- Risk Assessment
- Structured Pen Testing

Known Vulnerability

A known vulnerability if a vulnerability listed in the National Vulnerability Database (NVD). https://nvd.nist.gov

- Provides an ability to identify the software supply chain

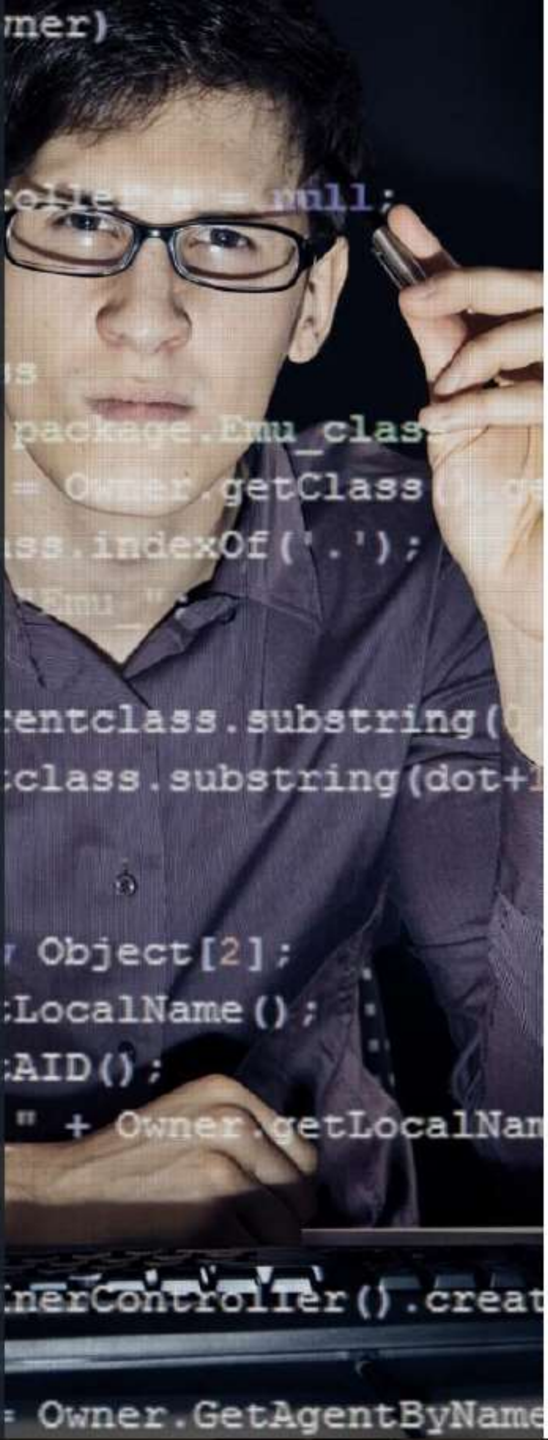
SOFTWARE BILL OF MATERIALS

Source of the software:

- In-house development
- Third-party library
- Open source
- Snippets of open source

UL 2900

- Fuzz Testing
- Known Vulnerability
- Code & Binary Analysis
- Access Control & Authentication
- Cryptography
- Remote Communication
- Software Updates
- Risk Assessment
- Structured Pen Testing



Static Analysis

A process in which source code, bytecode or binary code is analyzed without executing the code.

Analysis of:

- Source code
- Binary code
- Bytecode

UL 2900

Fuzz Testing

Known Vulnerability

Code & Binary Analysis

Access Control & Authentication

Cryptography

Remote Communication

Software Updates

Risk Assessment

Structured Pen Testing

FOUNDATIONAL SECURITY REQUIREMENTS FOR ANY PRODUCT

Testing Access Controls
- Recording Communication Logs
- Testing Logging Capabilities
- Verifying Products are setup for the controls listed

Cryptographic Controls
Verifying Cryptographic Controls Being Used

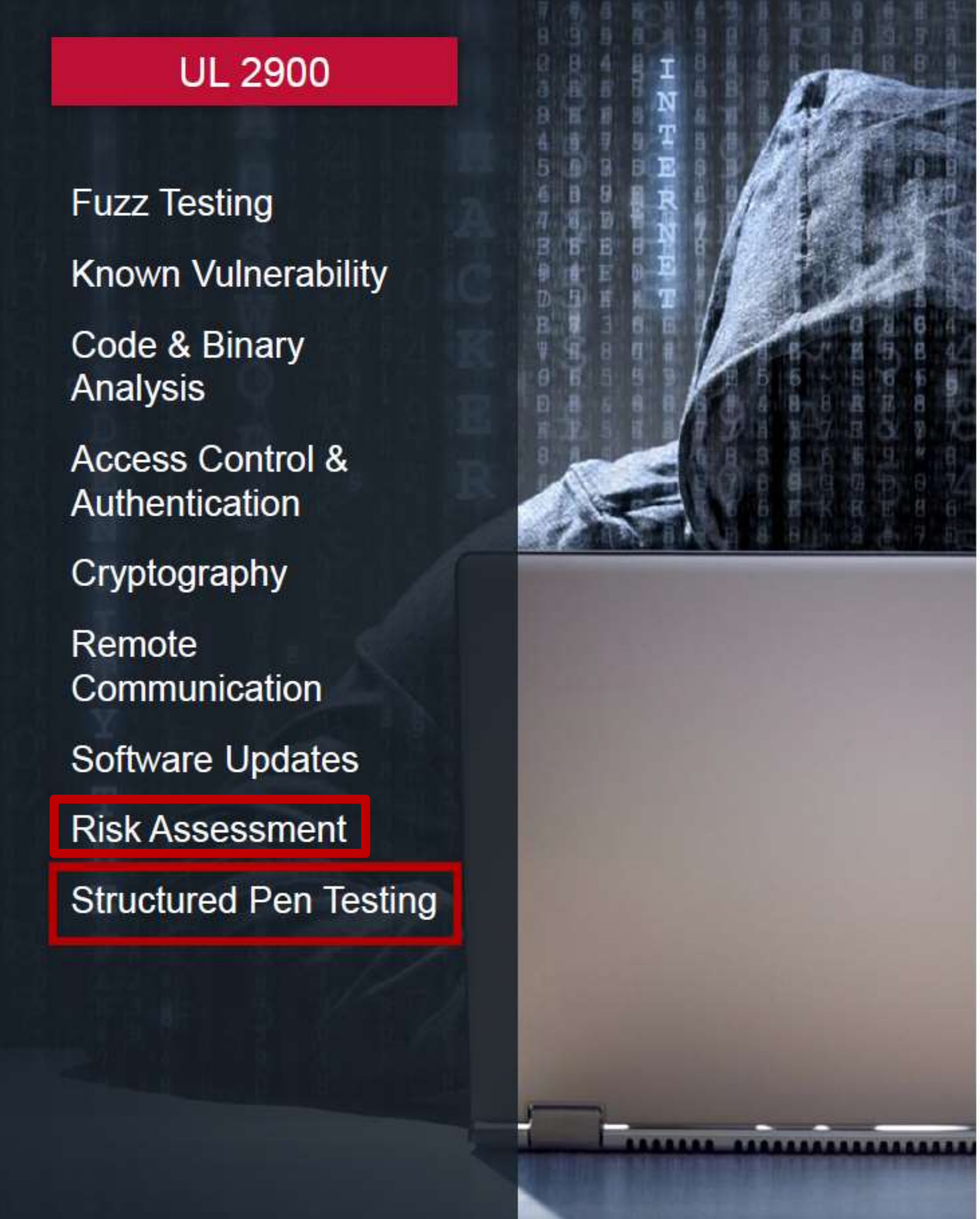
Remote Communication
Data communicated over any remote interface

Software Updates
Update software versions

UL 2900

- Fuzz Testing
- Known Vulnerability
- Code & Binary Analysis
- Access Control & Authentication
- Cryptography
- Remote Communication
- Software Updates
- Risk Assessment
- Structured Pen Testing

- Product management relates to the ability to perform an update of the software
- Requirements include:
  - Software update authenticity
  - Software update authorization
  - Software roll-back
  - Security logging
  - Management of configuration data (Zeroization)



UL 2900

- Fuzz Testing
- Known Vulnerability
- Code & Binary Analysis
- Access Control & Authentication
- Cryptography
- Remote Communication
- Software Updates
- Risk Assessment
- Structured Pen Testing

Structured Penetration Testing

A software attack on a computer system that looks for security weaknesses, potentially gaining access to the computer's features and data. The process typically identifies the target systems and a particular goal, then reviews available information and undertakes various means to attain the goal.

NOTE:
Penetration test will always be customized and structured to the specific product being tested as it is dependent on all the previous testing (CWE’s and CVEs) and the risk assessment.

Cybersecurity baseline for healthcare

Uses Existing Risk Management Processes

- ISO 14971 Product-centric risk management
- IEC 80001 Network-centric risk management

Uses Existing QMS

- ISO 13485 Quality management
- ISO 27000 Security management

Uses Existing SDLC

- IEC 62304 Medical device life cycle processes
- ISO 15408 Secure development lifecycle processes

Aligned With Regulatory Processes

- FDA Pre- and Post-Market Guidance
- ISO 15026 Assurance Case Structure

CAP tools help establish BOM showing software components from libraries and SOUP

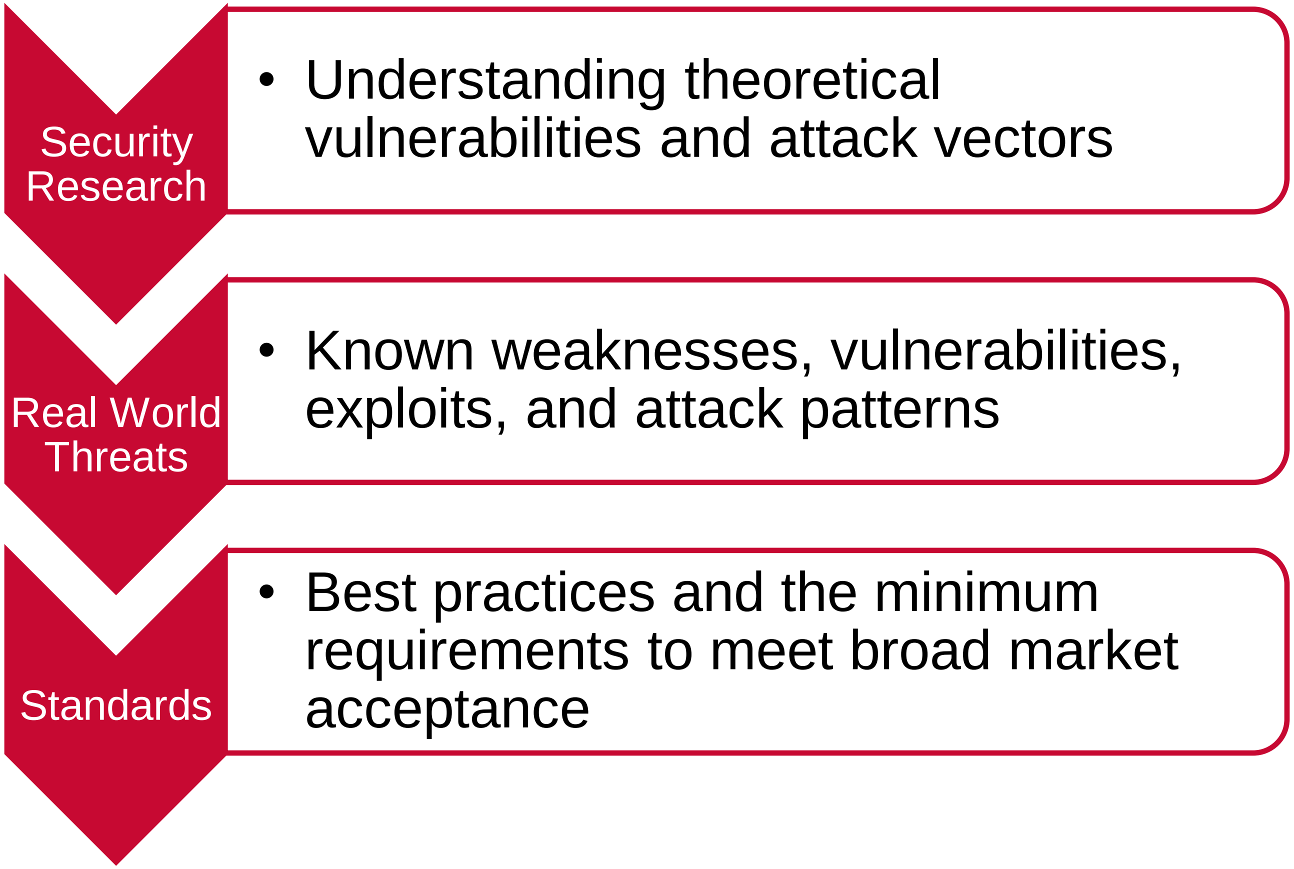
Manage patches

NIST CSF
NVD CVSS,
CWSS,
CAPEC, etc

Intended to help with hospital procurement processes to:

- reduce vulnerabilities
- reduce malware
- increase security awareness and preparedness

Building expectations in the market that all connectable products meet a minimum level of “hygiene” that continues to evolve as the threat landscape changes.



Security Research

- Understanding theoretical vulnerabilities and attack vectors

Real World Threats

- Known weaknesses, vulnerabilities, exploits, and attack patterns

Standards

- Best practices and the minimum requirements to meet broad market acceptance

Thank you